I/WE CLAIM:

1. A method for generating a cryptographic key, comprising steps of:

   using a sensor to acquire an image of a biometric feature of a user;

   generating binary output from analog signals output by the sensor; and

   generating the cryptographic key from the binary output using a selection algorithm.

2. A method as claimed in claim 1 wherein the step of generating is performed using a secret algorithm for selecting, arranging, and performing operations on the binary output.

3. A method as claimed in claim 2 wherein the encryption key is a key for a private key cryptographic system.

4. A method as claimed in claim 3 wherein the step of extracting comprises steps of:

   receiving the image in an analog signal format;

   passing the analog signal through an analog filter to remove gray scale from the analog signal; and

   converting the filtered analog signal to a binary output signal.

5. A method as claimed in claim 4 wherein the step of using a sensor comprises steps of:

   receiving electromagnetic radiation from the biometric feature at a charge coupled device; and

acquiring an image of the biometric feature.

6. A method as claimed in claim 5 wherein the biometric feature is a pattern located on a predefined surface area of a body and the step of deriving further comprises an initial step of measuring a life sign indicator of the surface area of the body in order to verify that the image is of a living being.

7. A method as claimed in claim 4 wherein the cryptographic key is derived from values extracted from the binary output that are unrelated to information used to classify or identify the biometric feature, so that the information cannot be used to associate the cryptographic key with the biometric feature.

8. A method as claimed in claim 4 further comprising a step of forwarding an IBS to a processor that stores a decryption algorithm for use with the cryptographic key to decrypt messages addressed to the user.

9. A method as claimed in claim 8 wherein the processor has access to a decryption algorithm that uses the IBS as the cryptographic key, and the method further comprises a step of using the IBS to authenticate the user by determining if the IBS matches a reference bit string, prior to decrypting the message.

10. A method as claimed in claim 9 wherein the processor resides on a smart card, and the method further comprises an initial step of inserting the smart card into a card reader that is adapted to receive both the message and the IBS.

11. A method as claimed in claim 8 wherein the step of generating is performed by the processor, and comprises steps of:

receiving the IBS; and

applying a transformation algorithm to the IBS to generate the cryptographic key.

12. A method as claimed in claim 11 wherein the step of generating further comprises a step of using the IBS to authenticate the user by verifying that the IBS matches a reference bit string, prior to the step of applying.

13. A method as claimed in claim 12 wherein the processor resides on a smart card that stores a decryption algorithm that uses the cryptographic key, and the method further comprises an initial step of inserting the smart card into a card reader provisioned with a memory for receiving the IBS and the message.

14. An apparatus for decrypting an encrypted message addressed to a user, the apparatus comprising a processor adapted to use an IBS derived from an image of a biometric feature of the user in conjunction with a decryption algorithm to decrypt the encrypted message.

15. An apparatus as claimed in claim 14 wherein the processor is adapted to use the IBS as a cryptographic key to decrypt the message using the decryption algorithm.

16. An apparatus as claimed in claim 15 wherein the processor is further adapted to first authenticate the user by matching the IBS with a reference bit string prior to decrypting the message.

17. An apparatus as claimed in claim 14 wherein the processor is further adapted to:

use the IBS to authenticate the user, by matching the IBS with a reference bit string associated with the user;

if the user is authenticated, apply a transformation algorithm to the IBS in order to generate a cryptographic key; and

decrypt the message using the cryptographic key and a decryption algorithm.

18. An apparatus as claimed in claim 17 wherein the processor resides on a smart card that stores the transformation algorithm, the decryption algorithm, and the reference bit string.

19. An apparatus as claimed in claim 18 wherein the smart card is docked at a card reader adapted to interface with both a sensor system, from which the IBS is received, and a communications processor from which the message is received.

20. An apparatus for generating a cryptographic key comprising a sensor system adapted to:

capture an image of a biometric feature of a user; and

extract from the image an identity bit string (IBS) used to generate the cryptographic key.

21. An apparatus as claimed in claim 20 wherein the sensor system comprises an integrated circuit adapted to generate the cryptographic key by selecting, arranging, and performing operations on the IBS using a selection algorithm.

22. An apparatus as claimed in claim 21 wherein the cryptographic key is a key for a private key cryptographic system.

23. An apparatus as claimed in claim 21 wherein the sensor system further comprises a sensor for generating an analog signal representative of the image of the biometric feature, and wherein the integrated circuit further comprises:

an analog filter adapted to eliminate gray scale from the analog signal;

a converter adapted to convert the filtered analog signal to binary output; and

a selection algorithm adapted to extract the IBS from the binary output.

24. An apparatus as claimed in claim 23 wherein the sensor comprises a charge coupled device (CCD) adapted to generate the analog signal in response to electromagnetic radiation, and the biometric feature comprises a predefined surface area of a user's body.

25. An apparatus as claimed in claim 24 wherein the sensor is adapted to capture an image of a

fingerprint, and the sensor area further comprises means for acquiring at least one measurement indicating that a finger placed on the sensor area is the finger of a living being.

26. A method as claimed in claim 23 wherein the cryptographic key is derived from values, and relations of values derived from the analog signal that are unrelated to information used to classify and identify the biometric feature, so that such information cannot be used to associate the cryptographic key with the biometric feature.

27. An apparatus as claimed in claim 23 wherein the integrated circuit comprises:

a circuit for generating an IBS by selecting, arranging, and performing operations on values obtained from the binary output using a predefined selection algorithm; and

a circuit for sending the IBS to a processor.

28. An apparatus as claimed in claim 27 wherein the processor is further adapted to generate the cryptographic key from the IBS by applying a transformation algorithm to the IBS.

29. An apparatus as claimed in claim 28 wherein the processor resides on a smart card, and the apparatus further comprises a card reader, the smart card being adapted to:

receive the IBS from the integrated circuit, via the card reader;

determine if the IBS matches a reference bit string associated with the user, to authenticate the user;

if the user is authenticated, to apply the transformation algorithm to the IBS to generate the cryptographic key; and

apply a decryption algorithm to the message using the cryptographic key.

30. A method for encrypting a message addressed to a user comprising a step of applying an encryption algorithm to the message using an encryption key derived from binary output generated from an analog signal associated with an image of a biometric feature of the user.

31. A method as claimed in claim 30 further comprising a step of:

authenticating the user by comparing the IBS with a reference bit string uniquely associated with the sender.

32. A method as claimed in claim 31, further comprising a step of inserting a smart card into a card reader, the card reader being adapted to convey the IBS to the smart card.